

1 November 2012

Draft DIGITALEUROPE amendments

Amendment 1

Recital 23 (Data Subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.</p>	<p>The principles of protection should apply <i>only</i> to any <i>specific</i> information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken: of all the <i>(i) only of those</i> means likely reasonably to be used either by the controller or by any other <i>natural or legal</i> person to identify the individual, <i>and (ii) of the reasonable likelihood of a person being identified.</i> The principles of data protection should not apply to data rendered anonymous <i>or made unreadable</i> in such a way that the data subject is no longer <i>or not yet</i> identifiable <i>from the data.</i></p> <p><i>Serial numbers of products, IP addresses, International Mobile Equipment Identity codes or other such identifiers should not be regarded as personal data before a link to a natural person can be established. Such identifiers should still not be regarded as personal data even after establishment of such link when they remain standalone in the possession of a controller or processor, i.e. when they are not combined with additional data in order to identify or target activities at a natural person.</i></p> <p><i>Where business contact information, such as names, surnames, professional addresses, emails, phone, fax numbers, is solely used or processed in a clearly defined business context, relating to a company and not an individual, this Regulation will not apply.</i></p>

Justification

Whether or not a person is identifiable should not be determined on the basis of a third party's means to identify the individual. Furthermore it should be made clear that the theoretical possibility to identify an individual is in itself not sufficient for considering an individual as identifiable. An overly broad definition of 'data subject' encompassing those identifiers (such as serial numbers etc.) which are not connected to a natural person does not lead to a better protection; on the contrary it takes away incentives to make data anonymous or to refrain from linking it to a natural person.

In line with an approach of the Spanish Data Privacy Authority, business contact information should be excluded from the Regulation's scope in certain cases. However, it is essential that the processing of contact information fulfils two requirements in order to be exempt from the scope. Firstly that the data processed is limited to what is merely necessary to identify the person within the company and secondly that the inclusion of contact information must be purely accidental or incidental regarding the real aim sought by the data processing, which is related not to the individual, but to the company where the person works.

Amendment 2

Recital 24 (Definition of Personal Data)	
Commission proposal	Proposed DIGITALEUROPE amendment
When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.	When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.

Justification

Online identifiers and location data on their own cannot identify individuals and cannot be considered as being personal data. Deleting "as such" indicates that online identifiers and location data can be considered as personal data when combined with other relevant information.

Amendment 3

Recital 25 (Consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>	<p>1. Consent should be given—<i>explicitly unambiguously</i> by any appropriate method <i>within the context of the product or service being offered</i> enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>

Justification

The term 'unambiguous' is better suited as it does not lower but rather increases the requirements of 'consent' compared to 'explicit' (because of the combination with the requirement of 'affirmative action') and it has a much better chance to be understood in a consistent way in all the Member States.

Amendment 4

Recital 27 (Main Establishment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.</p>	<p>The main establishment of a controller <i>and of a processor</i> in the Union should be determined <i>by the data controller and data processor respectively. Such determination should be made and evaluated</i> according to <i>the following</i> objective criteria: <i>the location of the group's European headquarters, the location of the company within the group with delegated data protection responsibilities, the location of the company which is best placed (in terms of management function, administrative burden etc) to deal with and enforce the rules as set out in this Regulation, the place where</i> and should imply the effective and real exercise of management activities determining the main-most decisions as to the purposes <i>or</i> conditions and means of processing <i>are taken</i> through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.</p>

Justification

The determination of the main establishment should be done on the basis of various criteria to ensure organisations have enough guidance to determine their main establishment and provide objective measures by which to judge their decision in the event of a dispute. Already there are such criteria to determine the lead DPA in the context of Binding Corporate Rules (BCRs) which have a proven track record. We think inserting the same criteria as outlined in Art 29 WP opinion 108 would provide more clarity and options that would not be covered under the current proposal. Moreover, as many entities are both controllers and processors,

we believe that they should be subject to the same set of criteria in determining their main establishment to avoid potentially conflicting results. For the same reason, we have changed “main” decisions to “most” as this would bring it in line with the BCR guidance.

Amendment 5

Recital 28 (Main Establishment)	
Commission proposal	Proposed DIGITALEUROPE amendment
A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. <i>A group of undertakings may nominate a single main establishment in the Union.</i>

Justification

The amendment clarifies that a group of undertakings can be viewed as a single entity responsible to a single supervisory authority. The simplification achieved by nominating a single point of contact should not be undermined by various supervisory authorities viewing individual controlled undertakings as separate data controllers or processors.

Amendment 6

Recital 34 (Consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment	Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller, <i>resulting in the data subject not having a true option of refusal without being subject to harmful consequences, taking into account the interest of the data subject. Such situations may exist, among others, in relation to</i>

context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	<i>certain aspects of employment relationship, in context of essential services or when dealing with public authorities. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</i>
--	--

Justification

Only when a data subject would suffer harmful consequences, taking into account the interest of the data subject, should consent be excluded as a valid legal ground for processing. There will be instances where in an employer – employee relationship, consent should be deemed a valid ground as a refusal by the employee would not have any harmful consequences.

Amendment 7

Recital 39 (Processing of Data for Network Security Purposes)	
Commission proposal	Proposed DIGITALEUROPE amendment
The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and	The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of public or private electronic communications

services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.	networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller <i>and vital interest of the data subject</i> . This could, for example, include preventing unauthorised access to <i>public or private</i> electronic communications networks and malicious code distribution and stopping <i>‘denial of service’</i> attacks and damage to computers and or electronic communication systems.
--	--

Justification

To maintain network and information security and protect the users’ terminals, it may be so that in specific cases personal data needs to be processed. Such processing is in the legitimate interest of the data controller and vital interest of the data subject and should be perceived as grounds for lawful processing under Article 6.1 (d) and 6.1 (f). We welcome the clarification and we support the intent of recital 39.

Amendment 8

Recital 49 (Processing of Data for Network Security Purposes)	
Commission proposal	Proposed DIGITALEUROPE amendment
The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.	<p>The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. <i>Except when processing data strictly necessary for the purposes of ensuring network and information security</i>, where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.</p> <p><i>In cases of threats to network and information security, a reasonable period for the obligation to explicitly inform the data subject on the legitimate interests pursued would be after the conclusion of the investigation at hand or once effective</i></p>

	<p><i>security is restored and the data subject can be identified, taking into account article 10. Should the investigation involve competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the responsibility for exercising the rights of the data subject will pass to the authorities in question.</i></p>
--	--

Justification

In certain situations in networking and information security processing where it is possible to identify the data subject (for example, an ISP which has a direct relationship with their subscribers and can map IP addresses to individuals), it is preferable to undertake certain processing without informing the data subject at the time, such as when there is a compromised machine sending spam and other circumstances where one is using the data to track the control traffic and identify the real malicious actors further up the chain. Hence a reasonable time period for informing the data subject that their personal data has been processed (in accordance with Article 14.4(b)) is after the conclusion of such investigations.

If the data subject in question is a suspected malicious actor and the suspected offence is criminal, you may not want to prejudice investigations by law enforcement authorities, and hence the responsibility to exercise the data subjects' rights in such situations should pass over to the authorities in question.

Furthermore, given that security companies may need to cooperate during investigations (e.g. a network security company and an ISP), the proposed requirement to inform the data subject at the point another recipient is informed could lead to data subjects being informed too early in the process and hence it should be deleted or an exception made when data is processed for network and information security purposes.

Amendment 9

Recital 51 (Right of access for the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain	Any person should have the right of access to personal data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to

communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	know and obtain communication in particular for what purposes the <i>personal</i> data are processed, for what period, which recipients receive the <i>personal</i> data, what is the logic of the <i>personal</i> data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including <i>for example</i> trade secrets <i>such as algorithms used, protection of network and information security,</i> or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.
---	--

Justification

The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified as it should not be used to gain access to specific trade secrets such as algorithms, nor impede with legitimate interests such as protecting users' terminals. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services.

In line with proposed amendments to Article 20, no specific additional requirement for "profiling" is required.

Amendment 10

Recital 52 (Right of access for the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	The controller should use all —reasonable measures <i>within the context of the product or service being provided, or otherwise within the context of the relationship between the controller and the data subject, and the sensitivity of the personal data being processed</i> to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain <i>nor</i>

	<i>be forced to gather</i> personal data for the unique purpose of being able to react to potential requests.
--	---

Justification

In some cases, complying with a right of access requirement will have as a consequence that the data controller will need to gather (more) personal data from the data subject in order to comply with the request. For example, data such as an IP address or an online identifier, that based on the context of the specific processing isn't personal data if the data controller can't by all means likely reasonably identify the data subject, would now become personal data as the data controller would need to collect more personal information as to verify the identity of the data subject, including gathering his IP address or online identifier and connecting as to authenticate that the person who is requesting access is actually the legitimate person. In line with the principle of data minimization, the Regulation should strive to avoid any additional requirements which impose on the data subject the obligation to do so. In addition, requiring "all" reasonable measures be used to verify identity would require multiple types of identity verification which may not be reasonable or practical, especially in cases where the sensitivity of the personal data being processed is low.

Amendment 11

Recital 58 (Profiling)	
Commission proposal	Proposed DIGITALEUROPE amendment
Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.	<i>Every natural</i> ———— <i>person A</i> <i>data subject</i> should <i>have the right</i> not <i>to</i> be subject to a measure which is based on profiling by means of automated processing, <i>which produces legal effects that gravely and adversely affect his fundamental rights. Depending on the context this may include processing aimed at evaluating, analysing or predicting a natural person's performance at work, economic situation, health, personal preferences, reliability or behaviour.</i> However, such measures should be allowed when <i>expressly</i> authorised by law, carried out in the course of entering or performance of a contract, <i>when necessary in a democratic society for the purposes of Article 21 or for the purposes of the</i>

	<i>legitimate interests pursued by a controller or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards as outlined in this Regulation. including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.</i>
--	--

Justification

In line with proposed amendments to Article 20.

The prohibition of profiling of a child was deleted in the final adopted Commission proposal as it was recognized that particularly in the online world, data subjects and their identity and consequently age, are not always identifiable by the controller.

Amendment 12

Recital 61 (Data Protection by Design/Default)	
Commission proposal	Proposed DIGITALEUROPE amendment
The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.	<i>To meet consumer and business expectations around the protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are may be taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures. which meet in particular the principles of data protection by design and data protection by default. Measures having as an objective the increase of consumer information and ease of choice shall be encouraged, based on industry cooperation and favouring innovative solutions, products and services.</i>

Justification

Privacy by Design/Default (PbD/D) are concepts currently being discussed internationally, relates to internal privacy and data protection processes of organizations and are based on a number of factors including their business models, size and interaction with personal data. Although every organization should strive to integrate privacy and data protection into its internal processes, the actual way it does so should remain flexible and leave room for adaptation based on the factors above. This is to say that there is no one right way, which is especially true in the case of SMEs and for entities that are far removed from processing identifiable personal data. It is essential that any PbD concept be technology-neutral and not introduce specific technology or operational mandates, or contribute to a differentiation between ICT and other economic sectors.

To avoid lack of consistency throughout the proposed text, it is important to streamline the proposed language for Art. 23 with other Data Protection by Design/Default-type obligations, which cover to large extends the proposed text, e.g. Art. 22 and Art. 5 c), Art. 26 (processor agreements), Art. 28 (documentation), Art. 30 (security), Art. 33 (data protection impact assessment) and Art. 35 (data protection officer).

The PbD/D concepts should therefore focus on designing privacy into processes and organizations and should maintain as a key objective providing consumers with appropriate tools to make an informed choice, but avoid creating additional uncertainties via unclear obligations, definitions and terms. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies to flourish in the spirit of the European Digital Agenda. Finally, there is a clear need to look into the issue with a global perspective to avoid further fragmentation, taking stock of industry's own efforts and taking technology developments into account.

Amendment 13

Recital 62 (Controller/Processor)	
Commission proposal	Proposed DIGITALEUROPE amendment
The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

Justification

In line with proposed amendments to Art 24.

Amendment 14

Recital 65 (Controller/Processor)	
Commission proposal	Proposed DIGITALEUROPE amendment
In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	In order to demonstrate compliance with this Regulation, the controller or processor should document <i>different categories of each</i> processing operation under its responsibility . Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

Justification

In line with proposed amendments to Article 28.

Amendment 15

Recital 66 (Security of Processing)	
Commission proposal	Proposed DIGITALEUROPE amendment
In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of	In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. <i>The implementation by the controller and the processor of such measures and the execution</i>

processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.	<i>thereof which would require processing of certain data to increase network and information security, is in the legitimate interests of the data controller, the processor and, where applicable, a third party providing support in its implementation.</i> When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.
--	---

Justification

Data controllers and processors should ensure that they have the right organizational measures in place to ensure security of processing and hence, enhancing overall network and information security. Such measures could, for example, be targeted at preventing unauthorized access to electronic communications networks, malicious code distribution and stopping of attacks and damage to computer and electronic communication systems. Where the implementation and execution of such measures would require the processing of data to the extent necessary for purposes of ensuring network and information security by the data controller, processor or a third party, such processing should be deemed to be a legitimate interest for processing. Such processing would need to provide the necessary safeguards as outlined in the regulation where possible.

Amendment 16

Recital 67 (Breach Notification)	
Commission proposal	Proposed DIGITALEUROPE amendment
A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The	A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a material breach has occurred, the controller should notify the breach to the supervisory authority without undue delay. and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany

<p>individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>	<p>the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by the supervisory authority where applicable by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>
---	---

Justification

In line with proposed language to Art 31.

Amendment 17

Recital 70 (Privacy Impact Assessment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate</p>	<p>Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate</p>

<p>general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.</p>	<p>general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.</p>
--	---

Justification

It should be up to the data controllers to assess the impact to privacy as they will determine the purposes of the processing.

Amendment 18

Recital 74 (Privacy Impact Assessment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure</p>	<p>Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation. and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines</p>

which defines the nature of the processing and lays down appropriate safeguards.	<i>the nature of the processing and lays down appropriate safeguards.</i>
--	--

Justification

Consultation should take place between supervisory authorities and data controllers and processors where there is an indication that processing operations involve a high degree of specific risks to the rights and freedom of data subjects and the risky processing might not be in compliance with this Regulation. Requiring prior consultation in other instances within the framework of this legislation will go against the goals of achieving a more flexible system.

Amendment 19

Recital 129 (Delegated Acts)	
Commission proposal	Proposed DIGITALEUROPE amendment
In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data	In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts <i>in specific cases and</i> in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. <i>In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility</i>



protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

~~of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.~~

Appropriate industry-led measures and policies shall take due account of the principles of technology, service and business model neutrality so as to favour the free movement of personal data within the Union.

Justification

Same justification as amendment 63

The recitals need not lay down an exhaustive list of delegated acts and we therefore propose to delete and refer to the individual articles. The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that

can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 20

Recital 130 (Implementing Acts)	
Commission proposal	Proposed DIGITALEUROPE amendment
In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third	In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a

country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.	<p>processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.</p> <p><i>In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.</i></p>
--	--

Justification

The recitals need not lay down an exhaustive list of implementing acts and we therefore propose to delete and refer to the individual articles. The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 21

Article 2.1 (Material Scope)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	1. This Regulation applies to the processing of personal data wholly or partly by automated means, <i>without discrimination between such processing means</i> , and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Justification

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 22

Article 4.1 (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;	'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person-, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

Justification

Online identifiers and location data on their own cannot identify individuals and need to be removed from this list. Also, in view of the fact that the draft Regulation places new burdens

on data controllers and processors, it is important to have a clear definition for 'personal data'.

Amendment 23

Article 4.2(a) (NEW) (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
	<i>'identification number' means any numeric, alphanumeric or similar code typically used in the online space, excluding codes assigned by a public or state controlled authority to identify a natural person as an individual.</i>

Justification

The definition of the term 'identification number' would help avoid confusion and increase legal certainty of article 4.1.

Amendment 24

Article 4 (5) (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

Justification

The essential character of a controller is that they decide why data is being processed in the first place and retain overall responsibility for activities undertaken. How exactly this is done in practice, e.g. whether one set of equipment or processing method is used over another, is

not a prerequisite for such a role. Focusing on the determination of the purposes as the primary factor brings greater clarity to the distinction between controllers and processors.

Amendment 25

Article 4 (8) (definitions: consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	'the data subject's consent' means any freely given specific, informed and <i>unambiguous</i> explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

Justification

The term 'unambiguous' is better suited as it does not lower but rather increases the requirements of 'consent' compared to 'explicit' (in combination with the requirement of 'affirmative action') and it has a much better chance to be understood in a consistent way in all the Member States.

Amendment 26

Article 4 (13) (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union	'main establishment' means as regards the controller, the place of its establishment in the Union <i>the location as determined by the data controller or data processor on the basis of the following objective criteria: the location of the group's European headquarters, the location of the company within the group with delegated data protection responsibilities, the location of the company which is best placed (in terms of management function, administrative</i>



take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;	<i>burden etc) to address and enforce the rules as set out in this Regulation, the place where the main most decisions as to the purposes or conditions and means of the processing of personal data are taken. if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;</i>
--	---

Justification

The determination of the main establishment should be done on the basis of various criteria to ensure organisations have enough guidance to determine their main establishment and provide objective measures by which to judge their decision in the event of a dispute. Already there are such criteria to determine the lead DPA in the context of Binding Corporate Rules (BCRs) which have a proven track record. We think inserting the same criteria as outlined in Art 29 WP opinion 108 would provide more clarity and options that would not be covered under the current proposal. Moreover, as many entities are both controllers and processors, we believe that they should be subject to the same set of criteria in determining their main establishment to avoid potentially conflicting results. For the same reason, we have changed “main” decisions to “most” as this would bring it in line with the BCR guidance.

Amendment 27

Article 5 (Principles relating to personal data processing)	
Commission proposal	Proposed DIGITALEUROPE amendment
Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;	Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; <i>in particular, those mechanisms shall ensure that by default personal data are not made accessible</i>

<p>(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p>	<p><i>to an indefinite number of individuals.</i></p> <p>(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p>
---	---

Justification

The principle added by this proposed amendment is taken from Article 23. From a structural point of view and to preserve the specific principle of Art 23 (2), we propose to move the language into Art 5, establishing the “principles relating to personal data processing”.

Amendment 28

Article 6 (1) (Lawfulness of processing)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject;</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p>2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; <i>or as otherwise appropriate to manage or effectuate the relationship between the controller and data subject;</i></p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject;</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller <i>or by a third party</i>, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p>2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and</p>

<p>safeguards referred to in Article 83.</p> <p>3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) the law of the Member State to which the controller is subject.</p> <p>The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>	<p>safeguards referred to in Article 83.</p> <p>3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) the law of the Member State to which the controller is subject.</p> <p>The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>
---	---

Justification

The processing of personal data in the legitimate interest of third parties should be deemed lawful, provided that the interests or the rights and freedoms of the data subject are not overriding. Such provision was already a substantial part of Directive 95/46/EC and is still necessary, among others, for legitimate business purposes of credit or collection agencies.

Amendment 29

Article 7 (Conditions for consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.</p> <p>2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.</p> <p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p>	<p>1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.</p> <p>2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.</p> <p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is when, due to a significant imbalance between the position of the data subject and the controller, the data subject could not refuse his consent without suffering harmful consequences of a material nature attributable to the controller.</p>

Justification

The proposed deletion will simplify the Regulation without diminishing the requirements necessary to obtain consent and therefore the protection of data subjects. Article 4.8 already specifies that consent needs to be given unambiguously on an informed basis. This regulates in a crystal clear way that the consumer needs to be fully aware of what he/she gives his/her consent to.

'Consent' should continue to be an important justification allowing the procession of personal data. The proposal of the Commission risks to devalue the consent requirement to an empty shell as in practice in a vast majority of cases there will be a significant imbalance between the controller and the data subject (quasi all employer/employee and business/consumer relationships). It is therefore important to specify that consent is not a basis for data processing only when the imbalance is such that the data subject would suffer material harm as a consequence of not providing consent.

Amendment 30

Article 10 (Processing not allowing identification)	
Commission proposal	Proposed DIGITALEUROPE amendment
If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	If the data processed by a controller do not permit the controller, <i>through means used by the controller</i> , to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

Justification

The proposed insertion would further clarify Article 10 that a controller does not have to collect additional information about data subjects in order to identify them for the sole purpose of complying with any provision of the regulation.

Amendment 31

Article 14 (Information to the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;</p> <p>(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article</p>	<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;</p> <p>(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article</p>

<p>6(1);</p> <p>(c) the period for which the personal data will be stored;</p> <p>(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(f) the recipients or categories of recipients of the personal data;</p> <p>(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;</p> <p>(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.</p> <p>2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.</p> <p>3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.</p> <p>4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p>(a) at the time when the personal data are</p>	<p>6(1);</p> <p>(c) the period for which the personal data will be stored;</p> <p>(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(f) the recipients or categories of recipients of the personal data;</p> <p>(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;</p> <p>(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.</p> <p>2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.</p> <p>3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.</p> <p>4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p>(a) at the time when the personal data are</p>
---	---

<p>obtained from the data subject; or</p> <p>(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.</p> <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <p>(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or</p> <p>(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or</p> <p>(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or</p> <p>(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.</p> <p>6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with</p>	<p>obtained from the data subject; or</p> <p>(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, <i>except when processing data strictly necessary for the purposes of ensuring network and information security, including fraud prevention</i> if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.</p> <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <p>(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or</p> <p>(b) the data are not collected from the data subject and the provision of such information proves impossible, <i>impractical, or</i> or would involve a disproportionate effort <i>or would impair other legitimate interests of the controller or vital interests of the data subject;</i> or</p> <p>(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or</p> <p>(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.</p> <p>6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.</p> <p>7. The Commission shall be empowered to</p>
--	--

<p>Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.</p> <p>8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.</p> <p>8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
---	---

Justification

Having established that personal data may be processed for network and information security purposes based on the provisions in article 6 (1) d, e and f, the data controller must abide by the conditions to inform the data subject on the legitimate interests pursued and on the right to object (as well as being compliant with further rights such as the right of access). In situations in networking and information security processing where it is possible to identify the data subject (for example, an ISP which has a direct relationship with their subscribers and can map IP addresses to individuals), it is preferable to undertake certain processing without informing the data subject at the time, such as when there is a compromised machine sending spam and other circumstances where one is using the data to track the control traffic and identify the real malicious actors further up the chain. Hence a reasonable time period for informing the data subject that their personal data has been processed (in accordance with Article 14.4(b)) is after the conclusion of such investigations.

If the data subject in question is a suspected malicious actor and the suspected offence is criminal, you may not want to prejudice investigations by law enforcement authorities, and hence the responsibility to exercise the data subjects' rights in such situations should pass over to the authorities in question.

Article 14.4(b) also envisages the informing of data subjects at the latest at first point of contact with a further recipient of the data. Given security companies may need to cooperate during investigations (e.g. a network security company and an ISP), this clause could lead to data subjects being informed too early in the process and hence it should be deleted or an exception made when data is processed for network and information security purposes.

Amendment 32

Article 15 (Right of access for the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:</p> <p>(a) the purposes of the processing;</p> <p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> <p>(d) the period for which the personal data will be stored;</p> <p>(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any</p>	<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed <i>and</i> the controller <i>can reply to this request without gathering additional personal data, the controller</i> shall provide the following information:</p> <p>(a) the purposes of the processing;</p> <p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> <p>(d) the period for which the personal data will be stored;</p> <p>(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any</p>



<p>available information as to their source;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>available information as to their source;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p>3. <i>(NEW) The right of access shall exclude any information whose disclosure could prejudice the securing, protecting and maintaining the resiliency of one or more information systems, for example the algorithms used in the processing.</i></p> <p>3. 4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, and requirements and exceptions for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>4. 5. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
---	---

Justification

In some cases, complying with a right of access requirement will have as a consequence that the data controller will need to gather (more) personal data from the data subject in order to comply with the request. For example, data such as an IP address, that is based on the context of the specific processing isn't personal data if the data controller can't by all means likely reasonably identify the data subject, would now become personal data as the data controller would need to collect more personal information as to verify the identity of the data subject, including gathering his IP address as to authenticate that the person who is requesting access is actually the legitimate person. In line with the principle of data minimization, the Regulation should strive to avoid any additional requirements which impose on the data subject the obligation to do so. The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified as it should not be used to gain access to specific trade secrets such as algorithms, nor impede with legitimate interests such as protecting users' terminals. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services. Furthermore the reference to Art. 20 has been deleted for consistency with proposed amendment to Art 20.

Amendment 33

Article 17 (Right to be Forgotten and to erasure)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p>	<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p>

<p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p> <p>4. Instead of erasure, the controller shall restrict processing of personal data where:</p> <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;</p> <p>(b) the controller no longer needs the personal</p>	<p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p> <p>4. Instead of erasure, the controller shall restrict processing of personal data where:</p> <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the</p>
--	---

<p>data for the accomplishment of its task but they have to be maintained for purposes of proof;</p> <p>(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;</p> <p>(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).</p> <p>5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.</p> <p>6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.</p> <p>7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.</p> <p>8. Where the erasure is carried out, the controller shall not otherwise process such</p>	<p>data;</p> <p>(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;</p> <p>(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;</p> <p>(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).</p> <p>5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.</p> <p>6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.</p> <p>7. <i>(NEW) Requests for the rectification, erasure or blocking of data shall not prejudice processing that is necessary to secure, protect and maintain the resiliency of one or more information systems. In addition, the right of rectification and/or erasure or personal data shall not apply to any personal data that is required to be maintained by legal obligation or to protect the rights of the controller, processor, or third parties.</i></p> <p>7.8 The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.</p>
--	---

<p>personal data.</p> <p>9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:</p> <ul style="list-style-type: none"> (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4. 	<p>8.9 Where the erasure is carried out, the controller shall not otherwise process such personal data.</p> <p>9.10 The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:</p> <ul style="list-style-type: none"> (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.
---	---

Justification

In addition, there are circumstances where the right of the data subject to rectify or erase personal data should not apply – for example, in compliance with EU member states laws and other jurisdictions requiring maintenance of certain types of personal data for national security reasons, or for investigations of potential wrongdoing.

Amendment 34

Article 18 (Right to data portability)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.</p> <p>2. Where the data subject has provided the</p>	<p>1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of their data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.</p> <p>2. Where the data subject has provided the personal data and the processing is based on</p>

<p>personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p>	<p>consent or on a contract, the data subject shall have the right to transmit those personal data, <i>which are processed by electronic means and in a structured and commonly used format</i> and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p>
<p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>

Justification

Users should own their data and ask for it when they no longer wish to use it. It should be clear that portability refers to the data provided by the subject which is in a commonly used format. Standardizing the format of data risks storing more or less data than is required for the service in question, and also poses a risk to the security of that data – common keys become easier to break. Standardizing data formats would also hinder innovation, as current uses of data may not reflect future needs and practices.

Amendment 35

Article 20 (Measures based on profiling)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work,</p>	<p>1. Every natural person data subject shall have the right not to be subject to a measure which produces legal effects <i>that gravely and adversely affect his fundamental rights concerning this natural person or significantly affects this natural person</i>, and which is based solely on automated processing intended to evaluate, certain personal aspects relating to this natural</p>

economic situation, location, health, personal preferences, reliability or behaviour.	person or to analyse or predict the natural person's performance at work, economic situation, location , health, personal preferences, reliability or behaviour.
---	--

Justification

Additional, distinct measures for processing of personal data through automated means are only justified for cases where the measure produces legal effects; any other profiling that constitutes processing of personal data is normal processing and already subject to all the provisions of the Regulation. The list in article 20 needs to be a closed one.

Amendment 36

Article 22 (Responsibility of the controller)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.
2. The measures provided for in paragraph 1 shall in particular include:	2. The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;	(a) keeping the documentation pursuant to Article 28;
(b) implementing the data security requirements laid down in Article 30;	(b) implementing the data security requirements laid down in Article 30;
(c) performing a data protection impact assessment pursuant to Article 33;	(c) performing a data protection impact assessment pursuant to Article 33;
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);



<p>(e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>	<p>(e) designating a data protection officer pursuant to Article 35(1), if any.</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p> <p><i>Having regard to the state of the art, the nature of personal data processing and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself, appropriate and demonstrable technical and organizational measures should be implemented in such a way that the processing will meet the requirements of this Regulation and ensures the protection of the rights of the data subject by design.</i></p> <p><i>Such measures include, without limitation:</i></p> <p>a) <i>Sufficiently independent management oversight of processing of personal data to ensure the existence and effectiveness of the technical and organizational measures;</i></p>
---	--



	<p>b) <i>Existence of proper policies, instructions or other guidelines to guide data processing needed to comply with the Regulation as well as procedures and enforcement to make such guidelines effective;</i></p> <p>c) <i>Existence of proper planning procedures to ensure compliance and to address potentially risky processing of personal data prior to the commencement of the processing;</i></p> <p>d) <i>Existence of appropriate documentation of data processing to enable compliance with the obligations arising from the Regulation;</i></p> <p>e) <i>Existence of adequately skilled data protection organization or data protection officer or other staff supported with adequate resources to oversee implementation of measures defined in this article and to monitor compliance with this Regulation, having particular regard to ensuring sufficient organizational independence of such data protection officer or other staff to prevent inappropriate conflicts of interest. Such a function may be fulfilled by way of a service contract;</i></p> <p>f) <i>Existence of proper awareness and training of the staff participating in data processing and decisions thereto of the obligations arising from this Regulation;</i></p> <p><i>Upon request by the competent data protection authority, the controller or processor shall demonstrate the existence of technical and organizational measures.</i></p> <p><i>Group of undertakings may apply joint technical and organizational measures to meet its obligations arising from the Regulation.</i></p> <p><i>This article does not apply to a natural person processing personal data without</i></p>
--	--

	<i>commercial interest.</i>
--	-----------------------------

Justification

We believe all organizations engaged in the processing of personal data, including controllers and processors irrespective of their size, should be held accountable for implementing appropriate, demonstrable and effective technical and organizational measures to ensure compliance with the Regulation.

However, to avoid new types of burdens and modalities on organizations and data protection authorities alike resulting from the detailed and prescriptive proposal, a simpler, and outcomes based organizational accountability obligation should be introduced. To ensure optimal data protection, the Regulation should provide enough flexibility to allow different organizations to implement the most effective technical and organizational measures, fit for the nature and structure of each respective organization.

Accountability is a well-established principle of data protection, found in existing guidance such as the OECD Guidelines¹ and APEC Privacy Framework² and in the laws of for example Canada and Mexico. Regulators, industry and advocacy groups have further defined the essential elements of accountability³.

Essential elements of effective privacy programs include sufficient management oversight, policies, processes and practices to make the policies effective, risk assessment and mitigation planning procedures, adequately skilled data protection staff, awareness and training of staff, internal enforcement, issue response and remedies to those whose privacy has been put at risk. Such program should be tailored having regard to the type of the organization, the nature of the processed personal data and the state of the art of technologies and available methodologies, for example to carry out a data protection impact assessment. Implementing such Accountability concept in the Data Protection Regulation instead of opting for the antiquated prescriptive and straight-jacked set of compliance requirements as currently proposed would in practice lead to improved data protection and avoid unnecessary burden for controllers, processors and DPAs.

Amendment 37

Art 23 (Data Protection by Design/Default)

¹ http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

² http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ecsg_privacyframework.ashx

³ http://www.informationpolicycentre.com/accountability-based_privacy_governance/

Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>	<p><i>1. Having regard to the state of the art and, the cost of implementation and international best practices, appropriate measures and procedures may be implemented to extend technically feasible and effective to ensure the processing operation meets the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensures the protection of the rights of the data subject.</i></p> <p><i>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</i></p> <p><i>Such measures and procedures shall:</i></p> <ul style="list-style-type: none"> <i>(a) follow the principle of technology, service and business model neutrality</i> <i>(b) be based on global industry-led efforts and best practices</i> <i>(c) be flexible based on an entities' business model, size, and level of interaction with personal data</i> <i>(d) take due account of existing internationally recognised technical standards and regulations in the area of public safety and security</i>

<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>(e) <i>take due account of international developments</i></p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> <p><i>In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.</i></p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
---	--

Justification

Privacy by Design/Default (PbD/D) are concepts currently being discussed internationally, relates to internal privacy and data protection processes of organizations and are based on a number of factors including their business models, size and interaction with personal data. Although every organization should strive to integrate privacy and data protection into its internal processes, the actual way it does so should remain flexible and leave room for adaptation based on the factors above. This is to say that there is no one right way, which is especially true in the case of SMEs and for entities that are far removed from processing identifiable personal data. It is essential that any PbD concept be technology-neutral and not

introduce specific technology or operational mandates, or contribute to a differentiation between ICT and other economic sectors.

To avoid lack of consistency throughout the proposed text, it is important to streamline the proposed language for Art. 23 with other Data Protection by Design/Default-type obligations, which cover to large extends the proposed text, e.g. Art. 22 and Art. 5 c), Art. 26 (processor agreements), Art. 28 (documentation), Art. 30 (security), Art. 33 (data protection impact assessment) and Art. 35 (data protection officer).

The PbD/D concepts should therefore focus on designing privacy into processes and organizations and should maintain as a key objective providing consumers with appropriate tools to make an informed choice, but avoid creating additional uncertainties via unclear obligations, definitions and terms. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies to flourish in the spirit of the European Digital Agenda. Finally, there is a clear need to look into the issue with a global perspective to avoid further fragmentation, taking stock of industry's own efforts and taking technology developments into account.

Amendment 38

Article 24 (Joint Controllers)	
Commission proposal	Proposed DIGITALEUROPE amendment
Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Justification

Same as justification for Article 4 (5)

(The essential character of a controller is that they decide why data is being processed in the first place and retain overall responsibility for activities undertaken. How exactly this is done in practice, e.g. whether one set of equipment or processing method is used over another, is not a prerequisite for such a role. Focusing on the determination of the purposes as the primary factor brings greater clarity to the distinction between controllers and processors.)

Amendment 39

Article 26 (Processor)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with</p>	<p>1. Where a-processing operation is to be carried out on behalf of a controller <i>and would involve personal data that would permit the processor to reasonably identify the data subject</i>, the controller shall choose a processor providing sufficient <i>guarantees assurances</i> to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller</p> <p>(e) insofar as this is possible given the nature of the processing, create in</p>

the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;	(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;
(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.	(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	4. If a processor processes personal data <i>for purposes</i> other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.	5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and

	reporting.
--	-----------------------

Justification

The proposed text introduces a host of new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice. For example, a controller may want to ensure that additional sub-processors - which may be numerous – apply effective data protection. But it should be clear this does not mean they should assess each in turn prior to their employment. As the processor has the closer relationship, they are better placed to make such a judgment. In relation to handing over results at the end of processing, there may be no results as such to hand over if the data minimisation principle has been effectively applied. Making data available to the supervisory authority should be handled by the controller. Certain information may be subject to a confidentiality obligation under law or contract and hence a processor may not be at liberty to disclose such information to a supervisory authority. Moreover, such data should not be required to be transmitted on a regular basis as this would overburden authorities and further increase the administrative burden. Finally, Art 26(4) implies that the controller would need to provide very detailed instructions as to what personal data the processor shall process. In reality, this is often not the case, yet based on this article the processor would carry the liability for not receiving extremely detailed instructions from the controller. Where a processor does breach such instructions, it is logical that the processor is considered a controller in respect of that processing but there is no reason to include the original data controller as a joint controller in this instance.

Amendment 40

Article 28 (Documentation)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of <i>all the main categories of</i> processing operations under its responsibility.
2. The documentation shall contain at least the following information:	2. <i>Such</i> The documentation shall contain at least the following information:
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;



<p>(b) the name and contact details of the data protection officer, if any;</p> <p>(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;</p> <p>(g) a general indication of the time limits for erasure of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following</p>	<p>(b) the name and contact details of the data protection organization or data protection officer, if any;</p> <p>(c) the generic purposes of the processing, ,including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data. —,including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of personal data to a third country or an international organisation, ,including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), a reference to the documentation of appropriate safeguards employed;</p> <p>(g) a general indication of the time limits for erasure or data retention policy applicable to of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on the basis of a request outlining the reasons for requiring access to the documents, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following</p>
---	--

<p>controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. <i>To ensure harmonized requirements within Europe,</i> tThe Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--

Justification

Effective data protection requires that organisations have sufficiently documented understanding of their data processing activities. The documentation requirement in Art 28.2 remains at rather high level and appears to largely duplicate the notification provisions in Art. 14.

Instead of satisfying bureaucratic needs, the aim of the documentation should be to help controllers and processors meet their obligations. Companies have many ways of documenting their data processing environment and no specific method should be mandated. Often such documentation exists through multiple means. A very detailed documentation procedure would remain an almost instantly outdated snapshot of a constantly changing reality characterized by complex data processing arrangements in a multiparty environment. Controllers cannot maintain detailed documentation of the IT architecture of the processors. Accordingly, processors should have an obligation to maintain such documentation of their processing. It should be left to the controllers and processors – in agreement with the lead DPA - based on the Accountability principle to determine which documentation is adequate and best suited for specific processing activities to comply with this Regulation and achieve the desired protection.

Amendment 41

Article 29 (Co-operation with the supervisory authority)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	<i>1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on the basis of a request outlining the reasons for requiring access to the documents, to the supervisory authority.</i>

Justification

The additional paragraph has been taken from Art. 28 (3) as it fits better in this Article that determines the relationship with the supervisory authority.

Amendment 42

Article 30 (Security of Processing)	
Commission proposal	Proposed DIGITALEUROPE amendment

<ol style="list-style-type: none"> 1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies. 4. The Commission may adopt, where 	<ol style="list-style-type: none"> 1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies. 3. (NEW) The implementation by the controller and the processor of measures, as referred to in paragraphs 1 and 2, and the execution thereof which would require processing of certain data to increase network and information security, falls under Article 6 (1) f. 4. The Commission may adopt, where necessary, implementing acts for
---	--



necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:	specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:
(a) prevent any unauthorised access to personal data;	(a) prevent any unauthorised access to personal data;
(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;	(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;
(c) ensure the verification of the lawfulness of processing operations.	(c) ensure the verification of the lawfulness of processing operations.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Data controllers and processors should ensure that they have the right organizational measures in place to ensure security of processing and hence, enhancing overall network and information security. Such measures could, for example, be targeted at preventing unauthorized access to electronic communications networks, malicious code distribution and stopping of attacks and damage to computer and electronic communication systems. Where the implementation and execution of such measures would require the processing of data to the extent strictly necessary for purposes of ensuring network and information security by the data controller, processor or a third party, such processing should be deemed to be a legitimate interest for processing. Such processing would need to provide the necessary safeguards as outlined in the regulation where possible.

Amendment 43

Article 31 (Notification of a personal data breach to the supervisory authority)	
Commission proposal	Proposed DIGITALEUROPE amendment
Notification of a personal data breach to the supervisory authority	Notification of a personal data breach to the supervisory authority
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify	1. In the case of a material personal data breach, the controller shall without undue delay, after the establishment of the existence of a personal data breach, and, where feasible, not later than 24

<p>the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p> <p>2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.</p> <p>3. The notification referred to in paragraph 1 must at least:</p> <p>(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;</p> <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p>	<p>hours after having become aware of notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours. The notification of a personal data breach to the supervisory authority shall not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures may include those that render the data unintelligible, unusable or anonymised to any person who is not authorised to access it.</p> <p>2. Pursuant to point (f) of Article 26(2), the processor shall <i>without undue delay after the establishment of the existence and nature of a personal data breach</i> alert and inform the <i>appropriate controller or controllers.</i> controller immediately after the establishment of a personal data breach.</p> <p>3. <i>To the extent feasible given the timing of the notification and the circumstances of the personal data breach,</i> The notification referred to in paragraph 1 must at least:</p> <p>(a) describe the nature of the personal data breach including the categories and <i>approximate</i> number of data subjects concerned and the categories <i>and number</i> of data records concerned;</p> <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p>
--	--



<p>(c) recommend measures to mitigate the possible adverse effects of the personal data breach;</p> <p>(d) describe the consequences of the personal data breach;</p> <p>(e) describe the measures proposed or taken by the controller to address the personal data breach.</p> <p>4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.</p> <p>6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in</p>	<p>(c) <i>include any recommended measures for the data subject</i> to mitigate the possible adverse effects of the personal data breach;</p> <p>(d) describe the consequences of the personal data breach;</p> <p>(e) describe the measures <i>proposed or taken that have been or will be implemented</i> by the controller to address the personal data breach <i>and to mitigate its possible adverse effects</i>.</p> <p>4. The controller shall document <i>material any</i> personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must <i>be sufficient to</i> enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.</p> <p>6. The Commission may lay down the standard format of such notification to the supervisory authority, <i>and</i> the procedures applicable to the <i>filing of reports. notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein.</i></p>
--	--

accordance with the examination procedure referred to in Article 87(2).	Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
---	---

Justification

Timely notification of only material breaches to DPAs will allow DPAs to prepare themselves, should affected individuals contact the DPA, as well as allow the DPA to better understand the nature and frequency of breaches. An expectation of notification within 24 hours is unreasonable. The timing of reporting material breaches to the DPA should be flexible so as not to interrupt the organization's efforts to deal with a breach event. Organizations are always at liberty to seek guidance from DPAs in the event of a data breach.

We also deleted the reference to art 26 (2) f to bring it in line with our proposed changes in that article.

Amendment 44

Article 32 (Communication of a personal data breach to the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Communication of a personal data breach to the data subject</p> <ol style="list-style-type: none"> When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3). The communication of a personal data 	<p>Communication of a personal data breach to the data subject</p> <ol style="list-style-type: none"> When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3). The communication of a personal data

<p>breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.</p> <p>4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p> <p>6. The Commission may lay down the format of the communication notification to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall may include those that render the data unintelligible, unusable or anonymised to any person who is not authorised to access it.</p> <p>4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p> <p>6. The Commission may lay down the format of the communication notification to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--

Justification

Data breach notification is an important element in any mitigation strategy. Timely notification to individuals in cases of material breaches can help them prepare and take steps to protect themselves and mitigate against potential future harm resulting from the breach. Organizations are in the best position to determine whether, when and how to notify their customers when a data breach occurs and so flexibility around timing and method of notification is required to reflect different businesses and operations and the types of data breaches that may occur. The organizations will need to keep track of material breaches as part of the overall obligation of organizational measures, so this can be demonstrated to the supervisory authorities upon request.

Amendment 45

NEW Article (after Art 32) (Communication of a personal data breach to other organisations)	
Commission proposal	Proposed DIGITALEUROPE amendment
	<i>A controller that communicates a personal data breach to a data subject pursuant to Article 32 may notify another organisation, a government institution or a part of a government institution of the personal data breach if that organisation, government institution or part may be able to reduce the risk of the harm that could result from it or mitigate that harm. Such notifications can be done without informing the data subject if the disclosure is made solely for the purposes of reducing the risk of the harm to the data subject that could result from the breach or mitigating that harm.</i>

Justification

In many cases other organisations or government institutions are in a position to be able to assist in mitigating harm that may result to a data subject following a personal data breach if they are made aware of the breach and the circumstances surrounding the breach. For example, in certain cases a flag may be added to a consumer's account or a request may be sent to log in and change one's password.

Amendment 46

Article 33 (Data protection impact assessment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p>	<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behavior, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly that gravely and adversely affect the individual's fundamental rights;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p>

<p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p> <p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p> <p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p>	<p>scale;</p> <p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p> <p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p> <p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p>
--	---



<p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p>	<p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p>
<p>7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>

Justification

The DPIA obligation is problematic as it is currently proposed. The approach to single out types of processing, brand them as risky, and treat them differently from supposedly non-risky processing is dangerous and will not produce the desired results. We believe all processing of personal data should be planned appropriately prior to commencing the processing to ensure compliance with the Regulation. Organizations should be held accountable for applying risk identification and mitigation planning methodologies that are appropriate for the processing at hand. No specific type of DPIA should be mandated nor should the assessment obligation be reserved to any specific type of processing.

DPIA's are one method, among others, to achieve the ultimate objective of ensuring that risks to privacy have been identified and proper mitigations planned in a timely fashion. Today, depending on the size of the organization, tens, hundreds or even thousands of DPIAs of various kinds are made annually to identify risks and to plan mitigations thereof. Different types of assessments are needed to properly assess different activities. Organizations are constantly searching for best methodologies for such risk identification and mitigation planning. Such methodologies constantly evolve, through efforts by practitioners, academia and various standardization bodies, and such incremental improvement should not be hindered by mandating any specific type of assessment.

The proposal suggests that a DPIA would be needed in specific risky situations. Some of the activities listed in article 33 are standard processing for which such an assessment should not need to be submitted to a DPA for prior authorization or consultation. In the current online reality, processing of location data, user segmentation and other such practices, for example, described as potentially risky

in the proposal, are the norm rather than exception and do not necessarily pose any significant risk to individuals. Therefore they should be removed from the list of risky processing and, in accordance with our belief that all processing warrants planning to ensure compliance, we propose that the reference to risky processing should only relate to prior consultation obligations.

Given the fact that, according to art. 14, data subjects need to be informed of the data processing, an obligation to consult data subjects as part of the assessment appears misplaced and unnecessary. It would also likely result in compromising important trade secrets. To ensure appropriate protection for personal data when data subjects cannot be informed of the processing, we propose a limited prior consultation obligation to govern such instances (see below for our comments and proposal for prior consultation).

Amendment 47

Article 34 (Prior authorisation and prior consultation)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</p> <p>2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:</p>	<p>1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</p> <p>2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:</p>

<p>(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or</p> <p>(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.</p> <p>3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.</p> <p>4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.</p> <p>5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the</p>	<p>(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or</p> <p>(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.</p> <p>3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance. <i>Such a decision shall be subject to appeal in a competent court and it may not be enforceable while being appealed unless the processing results to immediate serious harm suffered by data subjects.</i></p> <p>4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.</p> <p>5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data</p>
--	---

supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

~~within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.~~

~~6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.~~

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

~~8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.~~

9. The Commission may set out **non mandatory** standard forms and procedures for prior authorisations **and consultations** referred to in paragraphs 1 **and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6.** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

A modern data protection law should not require mandatory ex-ante consultation of the authorities by data controllers. The role of data protection authorities should be to focus 'ex-post' on the consistent enforcement of the rules. See also the recommendation of the Article 29 Working Party in its Opinion 3/2010 paragraph 63.

Amendment 48

Article 35 (Designation of Data Protection Officer)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller and the processor shall designate a data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may</p>	<p>1. The controller and the processor shall designate a <i>data protection organization or</i> data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection <i>organization or data protection</i> officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies</p>

<p>designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the name and contact details</p>	<p>representing categories of controllers or processors may designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection organization or data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection organization or data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the name and contact</p>
--	---

<p>of the data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>	<p>details of the data protection organization or data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection organization officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>
--	---

Justification

There are clear benefits in having in place roles and responsibilities to ensure compliance. The proposal, however, appears overly detailed in describing the tasks of a data protection officer and it also fails to recognize that also other organizational structures may result in equally or even more effective data protection. Here again it will be much more effective to introduce the Accountability principle into the Regulation instead, as proposed by Amendment 30. In larger organizations it is not reasonable to expect that a single data protection officer would be involved in all issues relating to the protection of personal data. Often in larger organizations the data protection roles and responsibilities, ranging from requirements setting, implementation, training and awareness, incident response and oversight and reporting are rightfully decentralized across the organizations, while being bound together by a comprehensive data protection program. Without senior management support and a systematic approach to compliance management it is unlikely that such a mandatory advisory and monitoring role envisaged by the proposal will lead to desired outcomes.

Some requirements for data protection officers in the proposal may even be counterproductive. For example, creating a two year protected term in form of a job guarantee for a data protection officer creates incentives to outsource the role to an external service provider to balance the risk of an unsuccessful recruitment. As in-depth knowledge of the organization is a prerequisite for successful data protection, this could hardly be seen as a desired outcome in all cases. Organizational independence should also include flexibility in organizing the data protection resources in a way that provides sufficient objectivity and independence of oversight and escalation. It seems more likely that a senior executive with accountability for effective organizational measures and who is a member of

organizations senior management leads to more long-term impact on the organization than a data protection officer with more of a procedural role.

Defining the obligation to appoint a data protection officer based on the number of employees seems arbitrary. It would make more sense to base it on the nature of data processing or number of data subjects involved.

Amendment 49

Article 36 (Position of the data protection officer)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.</p> <p>2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.</p> <p>3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.</p>	<p>1. The controller or the processor shall ensure that the data protection organization or data protection officer is properly and in a timely manner involved in all significant issues which relate to the protection of personal data.</p> <p>2. The controller or processor shall ensure that tThe data protection organization or data protection officer shall performs the his or her performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.</p> <p>3. The controller or the processor shall support the data protection organization or data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.</p>

Justification

It is not possible for a company to ensure that someone act “independently” just as much as it is impossible for a company to ensure that someone act honestly. Instead, this should be an obligation on the DPO.

Amendment 50

Article 37 (Tasks of the data protection organization or data protection officer)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller or the processor shall entrust the data protection officer at least with the following tasks:</p> <p>a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> <p>b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</p> <p>c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</p> <p>(d) to ensure that the documentation referred to in Article 28 is maintained;</p> <p>(e) to monitor the documentation, notification and communication of</p>	<p>1. The controller or the processor shall entrust the <i>data protection organization or</i> data protection officer at least with the following tasks:</p> <p>a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation <i>and to document this activity and the responses received;</i></p> <p>b) to <i>develop, support and</i> monitor the implementation <i>of measures referred to in Article 22, and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</i></p> <p>c) to monitor <i>the implementation and application compliance with the Regulation of this, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</i></p> <p>(d) to ensure that the documentation referred to in Article 28 is maintained;</p> <p>(e) to monitor the documentation, notification and communication of</p>

<p>personal data breaches pursuant to Articles 31 and 32;</p> <p>(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;</p> <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;</p> <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.</p> <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.</p>	<p>personal data breaches pursuant to Articles 31 and 32;</p> <p>(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;</p> <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;</p> <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.</p> <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.</p>
--	--

Justification

In today's organizational reality a lot of everyday advice is given over the phone, in meetings, through email or instant messaging. Having an obligation to systematically document one's everyday interaction with supported business operations would generate a massive and disproportionate administrative burden. However, actual privacy impact assessments and similarly structured privacy reviews need to be documented.

It should be up to the organization to define how they decide to organize their data protection organization and business in general. The proposed regulation appears to envision a

centralized organization with full and sole control over its resources and organization, which is just one approach to reach compliance.

Amendment 51

Article 38 (NEW) (Codes of conduct)	
Commission proposal	Proposed DIGITALEUROPE amendment
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.	3. Associations and other bodies representing categories of controllers <i>or processors</i> in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

Justification

Article 38.2 of the draft proposal states that Associations and other bodies in one Member State represent both controllers and processors while submitting draft codes of conduct, whereas art 38.3 states that Associations and other bodies in several Member States represent only controllers. We believe that both controller and processor should be included.

Amendment 52

Article 39 (Certification)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing	1. The Member States and the Commission shall encourage, in particular at European level, the <i>voluntary</i> establishment of data protection certification mechanisms and of data protection seals and marks, <i>which shall be capable of global application and affordable. These mechanisms shall also be technology neutral and will be</i> allowing data subjects to quickly assess the level of data protection provided by controllers and processors. <i>Such mechanisms shall: The data</i>

<p>operations.</p>	<p>protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.</p> <ul style="list-style-type: none"> a) <i>contribute, amongst other means, to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations</i> b) <i>take due account of the nature and sensitivity of the personal data being processed</i> c) <i>take due account of existing security measures and regulations in the area of public safety and security</i> d) <i>follow the principles of technology, service and business model neutrality</i> e) <i>be elaborated in consultation with the supervisory authorities</i> f) <i>be based on industry-led efforts</i> g) <i>take due account of international developments</i> h) <i>In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.</i> i) <i>Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is</i>
--------------------	--

<p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.</p> <p>3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>	<p><i>compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications and consistent with international industry-led standardisation efforts.</i></p> <p><i>Independent third parties or industry self regulatory bodies shall be the facilitators of such voluntary data protection certification mechanisms and data protection seals and marks, with easy access for citizens being a top priority. The European Data Protection Board shall serve as an enforcement agent.</i></p> <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries, <i>provided such measures are technology neutral.</i></p> <p>3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>
---	--

Justification

Certification mechanisms and data protection seals and marks developed and managed by industry should be favoured, provided they remain voluntary and affordable, particularly for SMEs. Such certification mechanisms should be open to companies both inside and outside the EEA, in order to facilitate international data flows, and be elaborated in consultation with the relevant stakeholders. They should enable competition, be industry-driven and favour innovative solutions for consumers. Indeed, industry is able to adapt to new market realities at a faster pace than government, and government does not have the same competitive incentive to enforce proper use of certifications (e.g., icons or seals on web pages) as industry does. In the long term, a certification mechanism developed and managed by industry, with regulators having backstop regulatory authority, would help to reduce compliance burdens on operators and foster competitiveness.

Amendment 53

Article 42 (Transfers by way of appropriate safeguards)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.</p>	<p>1. Where the Commission has taken no decision pursuant to Article 41, <i>or decides that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5)</i>, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.</p>
<p>2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:</p> <p>(a) binding corporate rules in accordance with Article 43; or</p> <p>(b) standard data protection clauses adopted by the Commission. Those implementing</p>	<p>2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:</p> <p>(a) binding corporate rules in accordance with Article 43; or</p> <p>(b) standard data protection clauses adopted by the Commission. Those</p>

<p>acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or</p> <p>(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or</p> <p>(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.</p> <p>3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.</p> <p>4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.</p>	<p>implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or</p> <p>(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or</p> <p>(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.</p> <p>3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.</p> <p>4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.</p> <p><i>(a) A controller or processor may choose to base transfers on standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and to offer in addition to these standard clauses supplemental, legally binding commitments that apply to transferred data. In such cases, these additional commitments shall be subject to prior consultation with the competent</i></p>
---	--

<p>5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.</p>	<p><i>supervisory authority and shall supplement and not contradict, directly or indirectly, the standard clauses. Member States, supervisory authorities and the Commission shall encourage the use of supplemental and legally binding commitments by offering a data protection seal, mark or mechanism, adopted pursuant to Article 39, to controllers and processors who adopt these heightened safeguards.</i></p> <p>5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.</p>
--	---

Justification

The wording of the draft proposal could rule out all forms of data transfers to the country, territory, sector or international organization considered as not offering an adequate level of protection regardless of whether other appropriate safeguards are put in place. Article 41(6) of the draft proposal indeed provides that the prohibition to transfer personal data in case of

inadequacy decided by the Commission is “without prejudice to Articles 42 to 44,” while Articles 42(1) and 44(1) mention that they apply only if the Commission has not taken any decision on adequacy.

With the increasing globalisation of business and the evolution of computing models like the cloud, cross-border flows of personal data have become routine. In this environment, it is critical that controllers and processors apply strong safeguards to personal data regardless of where that data is located. Users will only have confidence in cloud computing if they know that their data is safe in the cloud. Helpfully, the Regulation already requires that transfers of personal data to third countries may only be carried out in full compliance with the Regulation. This is an important principle. But controllers and processors should be incentivised to go beyond the Regulation in some cases. Indeed, controllers and processors will often have direct and practical experience that demonstrates that additional safeguards -- i.e., safeguards that supplement those in the Regulation -- may be appropriate in relation to the personal data they are transferring. The Regulation should encourage these controllers and processors to offer supplemental safeguards where these are appropriate. The amendment proposed above would help to achieve this by allowing controllers and processors that base data transfers on standard data protection clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation to also offer additional protections to customers in the form of legally binding contractual commitments (e.g., data processing agreements) that expand on the standard clauses. In this way, controllers and processors can offer additional protections that reflect the ways in which they will be processing data and particular safeguards appropriate to that processing. Of course, these supplemental commitments should not contradict the standard clauses.

Amendment 54

Article 43 (Transfers by way of binding corporate rules)	
Commission proposal	<i>Proposed DIGITALEUROPE amendment</i>

<p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members;</p> <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> <p>(c) their legally binding nature, both internally and externally;</p> <p>(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;</p> <p>(e) the rights of data subjects and the means to exercise these rights, including the right</p>	<p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings and their external subcontractors, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members, and their external subcontractors;</p> <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> <p>(c) their legally binding nature, both internally and externally;</p> <p>(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;</p> <p>(e) the rights of data subjects and the means to exercise these rights, including the right</p>
--	---

<p>not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;</p> <p>(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;</p> <p>(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;</p> <p>(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;</p> <p>(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;</p> <p>(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;</p> <p>(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group</p>	<p>not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;</p> <p>(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;</p> <p>(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;</p> <p>(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;</p> <p>(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;</p> <p>(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;</p> <p>(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group</p>
--	--

<p>of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.</p> <p>4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>	<p>of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.</p> <p>4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>
---	---

Justification

In the Cloud Computing services, cloud providers often use the external subcontractors to perform a specific task to deliver 24/7 service and maintenance. Therefore, this should be recognised in the Binding Corporate Rules by the supervising authority.

Amendment 55

Article 44 (Derogations)	
Commission proposal	Proposed DIGITALEUROPE amendment

<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <ul style="list-style-type: none"> (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or (d) the transfer is necessary for important grounds of public interest; or (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or (g) the transfer is made from a register which according to Union or Member State law is intended to provide 	<p>1. In the absence of an adequacy decision pursuant to Article 41; <i>or where the Commission decides that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5); or in the absence</i> of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <ul style="list-style-type: none"> (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or (d) the transfer is necessary for important grounds of public interest; or (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any
--	--

<p>information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.</p> <p>3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p>	<p>person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.</p> <p>3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>4. Points (b), (c) and (h) of paragraph 1 shall</p>
--	---

<p>4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.</p> <p>5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.</p> <p>6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.</p>	<p>not apply to activities carried out by public authorities in the exercise of their public powers.</p> <p>5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.</p> <p>6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.</p>
--	--

Justification

See justification for proposed amendment to Article 42.

(The wording of the draft proposal could rule out all forms of data transfers to the country, territory, sector or international organization considered as not offering an adequate level of protection regardless of whether other appropriate safeguards are put in place. Article 41(6) of the draft proposal indeed provides that the prohibition to transfer personal data in case of inadequacy decided by the Commission is “without prejudice to Articles 42 to 44,” while Articles 42(1) and 44(1) mention that they apply only if the Commission has not taken any decision on adequacy.

With the increasing globalisation of business and the evolution of computing models like the cloud, cross-border flows of personal data have become routine. In this environment, it is critical that controllers and processors apply strong safeguards to personal data regardless of where that data is located. Users will only have confidence in cloud computing if they know that their data is safe in the cloud. Helpfully, the Regulation already requires that transfers of personal data to third countries may only be carried out in full compliance with the Regulation. This is an important principle. But controllers and processors should be

incentivised to go beyond the Regulation in some cases. Indeed, controllers and processors will often have direct and practical experience that demonstrates that additional safeguards -- i.e., safeguards that supplement those in the Regulation -- may be appropriate in relation to the personal data they are transferring. The Regulation should encourage these controllers and processors to offer supplemental safeguards where these are appropriate. The amendment proposed above would help to achieve this by allowing controllers and processors that base data transfers on standard data protection clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation to also offer additional protections to customers in the form of legally binding contractual commitments (e.g., data processing agreements) that expand on the standard clauses. In this way, controllers and processors can offer additional protections that reflect the ways in which they will be processing data and particular safeguards appropriate to that processing. Of course, these supplemental commitments should not contradict the standard clauses.)

Amendment 56

Article 51 (Competence)	
Commission proposal	Proposed DIGITALEUROPE amendment
<ol style="list-style-type: none"> Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation. 	<ol style="list-style-type: none"> Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States <i>and any disputes should be decided upon in accordance with the consistency mechanism set out in article 58, and this</i> without prejudice to the <i>other</i> provisions of Chapter VII of this Regulation. <i>Where a group of undertakings has nominated a single main establishment the</i>

<p>3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p>	<p><i>supervisory authority of that establishment shall be competent.</i></p> <p>3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p>
--	--

Justification

See justification under recital 27

(The determination of the main establishment should be done on the basis of various criteria to ensure organisations have enough guidance to determine their main establishment and provide objective measures by which to judge their decision in the event of a dispute. Already there are such criteria to determine the lead DPA in the context of Binding Corporate Rules (BCRs) which have a proven track record. We think inserting the same criteria as outlined in Art 29 WP opinion 108 would provide more clarity and options that would not be covered under the current proposal. Moreover, as many entities are both controllers and processors, we believe that they should be subject to the same set of criteria in determining their main establishment to avoid potentially conflicting results.)

Amendment 57

Article 53 (Powers)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Each supervisory authority shall have the power:</p> <p>(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;</p> <p>(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this</p>	<p>1. Each The competent supervisory authority pursuant to Article 51(1) or 51(2) shall have the power:</p> <p>(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;</p> <p>(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided</p>

<p>Regulation;</p> <p>(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;</p> <p>(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;</p> <p>(e) to warn or admonish the controller or the processor;</p> <p>(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;</p> <p>(g) to impose a temporary or definitive ban on processing;</p> <p>(h) to suspend data flows to a recipient in a third country or to an international organisation;</p> <p>(i) to issue opinions on any issue related to the protection of personal data;</p> <p>(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.</p> <p>2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:</p> <p>(a) access to all personal data and to all information necessary for the performance of its duties;</p> <p>(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.</p> <p>The powers referred to in point (b) shall</p>	<p>by this Regulation;</p> <p>(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;</p> <p>(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;</p> <p>(e) to warn or admonish the controller or the processor;</p> <p>(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;</p> <p>(g) to impose a temporary or definitive ban on processing;</p> <p>(h) to suspend data flows to a recipient in a third country or to an international organisation;</p> <p>(i) to issue opinions on any issue related to the protection of personal data;</p> <p>(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.</p> <p>2. Each The competent supervisory authority shall have the investigative power to obtain from the controller or the processor:</p> <p>(a) access to all personal data and to all information necessary for the performance of its duties;</p> <p>(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.</p>
---	--

<p>be exercised in conformity with Union law and Member State law.</p> <p>3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).</p> <p>4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).</p>	<p>The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.</p> <p>3. Each The competent supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).</p> <p>4. Each The competent supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).</p>
---	---

Justification

This change reinforces the notion of the lead supervisory authority and avoids a situation where there is confusion on the behalf of data controllers, data processors and the data protection authorities as to which body retains competence or where the competencies of the data protection authorities are overlapping in any particular situation.

Amendment 58

Article 58(4) (Opinion of the European Data Protection Board)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.</p> <p>2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:</p> <p>(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or</p>	<p>1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.</p> <p>2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:</p> <p>(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or</p>

<p>(b) may substantially affect the free movement of personal data within the Union; or</p> <p>(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or</p> <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> <p>3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p> <p>4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.</p> <p>5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.</p>	<p>(b) may substantially affect the free movement of personal data within the Union; or</p> <p>(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or</p> <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> <p>3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p> <p>4. In order to ensure correct and consistent application of this Regulation, the Commission may, <i>acting on its own behalf, and shall at the request of a stakeholder</i>, request that any matter shall be dealt with in the consistency mechanism. <i>The Commission shall, on an annual basis, provide an overview of the requests made by third parties.</i></p> <p>5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.</p>
---	--

<p>6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.</p> <p>7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.</p> <p>8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.</p>	<p>6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.</p> <p>7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.</p> <p>8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.</p>
--	--

Justification

When there are inconsistencies with regards to the application of the Regulation which threaten the harmonized implementation and affect specific stakeholders, the affected stakeholders should be given the right to bring their concerns into the consistency mechanism. We think the European Commission could play a central role in coordinating such requests.

Amendment 59

Article 66 (1) (Tasks of the European Data Protection Board)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:</p> <p>(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;</p> <p>(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;</p> <p>(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;</p> <p>(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;</p>	<p>1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative—or at the request of the Commission <i>or other stakeholders</i>, in particular:</p> <p>(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;</p> <p>(b) examine, on its own initiative or on request of one of its members or on request of the Commission, <i>or on request of stakeholders</i> any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;</p> <p>(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;</p> <p>(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;</p>

<p>(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;</p> <p>(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;</p> <p>(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.</p> <p>2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.</p> <p>3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.</p> <p>4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.</p>	<p>(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;</p> <p>(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;</p> <p>(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.</p> <p>2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.</p> <p>3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.</p> <p>4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.</p>
---	---

Justification

We would encourage the European Parliament to introduce mechanisms to make the Board more accessible and responsive to requests from other stakeholders including the European Parliament for topics that should be addressed by the Board as this is now only a prerogative

of the DPAs or the Commission. Therefore we are proposing language to give stakeholders such opportunities.

Amendment 60

Art 66 (5) NEW (Consultation of European Data Protection Board)	
Commission proposal	Proposed DIGITALEUROPE amendment
	<p><i>5. Where appropriate, the European Data Protection Board shall, in its execution of the tasks as outlined in article 66, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.</i></p>

Justification

Before the Board adopts opinions or reports, they should consult interested parties and give them the opportunity to comment within a reasonable period as possible for other regulatory domains (see BEREC example⁴).

Amendment 61

Article 77 (Right to compensation and liability)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the</p>	<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the</p>

⁴ Regulation on establishment of BEREC (1211/2009); articles 17 (Consultation) and 18 (Transparency) define how BEREC is interacting with public and interested parties.

processor for the damage suffered.	controller or the processor for the damage suffered.
2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.	2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage, <i>to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.</i>
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	3. The controller or the processor may be exempted from this the liability <i>under paragraph 2</i> , in whole or in part, if the <i>respective</i> controller or the processor proves that they are not <i>to be</i> responsible for the event giving rise to the damage.
	4. <i>If a processor processes personal data other than as instructed by the controller, they may be held liable should any person suffer damage as a result of such processing.</i>

Justification

Under the current Directive, liability is correctly attributed to the data controller. Essentially, they direct the data processor and if the processor does not act on those orders then contractual arrangements apply to address the circumstances. Introducing a vague liability clause does not clarify the current situation but creates confusion for controllers, processors and data subjects alike.

Amendment 62

Article 79 (Administrative sanctions)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.	1. Each <i>The competent</i> supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, ***the sensitivity of the personal data at issue***, the intentional or negligent character of the infringement, ***the degree of harm or risk of significant harm created by the violation***, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach. ***While some discretion is granted in the imposition of such sanctions to take into account the circumstances outlined above and other facts specific to the situation, divergences in the application of administrative sanctions may be subject to review pursuant to the consistency mechanism.***

In setting an administrative fine, supervisory authorities shall also take into account fines, damages or other penalties previously imposed by a court or other body on the natural or legal person in respect of the violation in issue.

(a) Aggravating factors that support administrative fines at the upper limits established in paragraphs 4 to 6 shall include in particular:

(i) repeated violations committed in reckless disregard of applicable law;

(ii) refusal to co-operate with or obstruction of an enforcement process; and

(iii) violations that are deliberate, serious

	<p><i>and likely to cause substantial damage.</i></p> <p><i>2b. Mitigating factors which support administrative fines at the lower limits shall include:</i></p> <p><i>(i) measures having been taken by the natural or legal person to ensure compliance with relevant obligations;</i></p> <p><i>(ii) genuine uncertainty as to whether the activity constituted a violation of the relevant obligations;</i></p> <p><i>(iii) immediate termination of the violation upon knowledge; and</i></p> <p><i>(iv) co-operation with any enforcement processes.</i></p>
<p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p>	<p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed. ,where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p>
<p>4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(c) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> <p>(d) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p>	<p>4. The supervisory authority shall <i>may</i> impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> <p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p>
<p>5. The supervisory authority shall impose a</p>	

<p>fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13; (c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; (d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; (e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24; (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 	<p>5. The supervisory authority <i>shall may</i> impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13; (c) does not comply with the right to be forgotten or to erasure <i>on websites or data within their control</i>, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; (d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; (e) does not or not sufficiently determine define the respective responsibilities with co-controllers pursuant to Article 24; (f) does not or not sufficiently take reasonable steps to maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (g) does not comply, in cases where special
---	---



<p>and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.</p>	<p>categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.</p>
<p>6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (c) does not comply with an objection or the requirement pursuant to Article 19; (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20; (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30; (f) does not designate a representative pursuant to Article 25; (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27; (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the 	<p>6. The supervisory authority shall<i>may</i> impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (c) does not comply with an objection or the requirement pursuant to Article 19; (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20; (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30; (f) does not designate a representative pursuant to Article 25; (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27; (h) does not <i>timely or completely</i> alert on or notify a personal data breach or does



data subject pursuant to Articles 31 and 32;	<i>not timely or completely notify the data breach</i> to the supervisory authority or <i>where required does not timely and appropriately notify the to the</i> data subject pursuant to Articles 31 and 32;
(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;	(i) <i>does not carry out a data protection impact assessment where required pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;</i>
(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;	(j) <i>does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;</i>
(k) misuses a data protection seal or mark in the meaning of Article 39;	(k) misuses a data protection seal or mark in the meaning of Article 39;
(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;	(l) carries out or instructs a data transfer or transfers to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;
(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);	(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);
(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);	(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);
(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.	(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.
7. The Commission shall be empowered to	

<p>adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>	<p>7. <i>Where convincing evidence exists of continued negligence or gross negligence by organisations in the execution of their responsibilities under this Regulation or the failure of these sanctions to deter serious abuses that cannot be addressed under the current framework</i> The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts <i>or conditions</i> of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>
--	---

Justification

DIGITALEUROPE believes that the excessively broad scope and scale of the fines are not commensurate with the associated offences, especially if they are not demonstrated to be intentional.

One of our main concerns is that according to the Regulation both negligent and intentional breaches give rise to fines. Much of the Regulation is new, with limited guidance as to how it should be implemented in practice. As such, in the first few years after the Regulation comes into force questions of interpretation will arise as to its meaning, intent and nuances. Therefore, we would recommend that article 79 is amended to limit fines to intentional non-compliance.

The amendments specify the mitigating and aggravating factors that supervisory authorities should consider when imposing fines. In doing so, the amendments ensure that higher fines are imposed on more serious misconduct, and also encourage compliance and co-operation once a violation is discovered. Specifying these factors will also promote greater consistency across the Member States in terms of the fines imposed.

Even if fines do become limited to intentional acts, we find the range of acts does not commensurate with the scale of fines. Open-ended fines such as 2% of world-wide turn over create open-ended risk that engenders uncertainty. It would be better if each category of fines were to be capped at a particular amount. We would also suggest that the percentage of turnover be retained within the capped amount in order to be fairer to SMEs. Thus a fine

structure may read fines up to 2% of worldwide turnover, but not exceeding, for example €500,000.

We would suggest guidance related to fines and their imposition. Furthermore, we disagree with the fact that the word 'shall' is used for every single fine envisaged in article 79, thus forbidding DPAs from exercising any discretion as to whether a fine should be imposed. We also believe that a coordinating mechanism would be appropriate to assure a reasonable level of correlation between violations and corresponding penalties across Member States.

Amendment 63

Article 86.6 (new) (Exercise of the Delegation)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p> <p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p> <p>3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the</p>	<p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p> <p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p> <p>3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the</p>

<p>European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p> <p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p> <p>5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.</p>	<p>European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p> <p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p> <p>5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.</p> <p><i>6(new). Acts adopted in accordance with this Article shall be technology neutral and non-discriminatory irrespective of the means used for the lawful processing of personal data.</i></p>
--	--

Justification

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 64

Article 87.4 (new) (Exercise of the Delegation)	
Commission proposal	Proposed DIGITALEUROPE amendment
<ol style="list-style-type: none"> 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. 3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply. 	<ol style="list-style-type: none"> 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. 3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply. <p><i>4(new). Acts adopted in accordance with this Article shall be technology neutral and non-discriminatory irrespective of the means used for the lawful processing of personal data.</i></p>

Justification

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

ABOUT DIGITALEUROPE

DIGITALEUROPE is the voice of the European digital economy including information and communication technologies and consumer electronics. DIGITALEUROPE is dedicated to improving the business environment for the European digital technology industry and to promoting our sector's contribution to economic growth and social progress in the European Union.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 global corporations and 37 national trade associations from across Europe. In total, 10,000 companies employing two million citizens and generating €1 trillion in revenues. Our website provides further information on our recent news and activities: <http://www.digitaleurope.org>

THE MEMBERSHIP OF DIGITALEUROPE

COMPANY MEMBERS:

Acer, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, Bang & Olufsen, BenQ Europa BV, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, JVC Kenwood Group, Kodak, Konica Minolta, Kyocera Mita, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Océ, Oki, Optoma, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, SAP, Sharp, Siemens, Smart Technologies, Sony, Sony Ericsson, Swatch Group, Technicolor, Texas Instruments, Toshiba, Xerox, ZTE Corporation.

NATIONAL TRADE ASSOCIATIONS:

Belgium: AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy:** ANITEC, **Lithuania:** INFOBALT; **Netherlands:** ICT OFFICE, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE, APDC; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AMETIC; **Sweden:** IT&TELEKOMFÖRETAGEN; **United Kingdom:** INTELLECT; **Belarus:** INFOPARK; **Norway:** IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE